HOMELAND SECURITY
COMMITTEE

Statement of Subcommittee Chairman John Ratcliffe (R-TX)
Cybersecurity and Infrastructure Protection Subcommittee

"Examining DHS' Efforts to Strengthen its Cybersecurity Workforce"

March 7, 2018

Remarks as Prepared

I would like begin by thanking our panel for taking the time today to testify. Your thoughts and opinions are very important as we oversee the implementation of workforce authorities at the Department of Homeland Security.

We have seen cyberattacks affect almost every facet of our daily lives with devastating impacts, and they remind us of how vulnerable governments and economies are to the very real threat that our cyber adversaries pose. As the lead civilian agency for our federal cybersecurity posture, the Department of Homeland Security is a key piece of this equation, especially the National Protection and Programs Directorate. A knowledgeable and skilled cybersecurity workforce at DHS is on the front lines of securing our federal networks and protecting critical infrastructure.

Against this backdrop, DHS must compete with the private sector to recruit and retain the best talent possible in order to carry out its cybersecurity mission and protect our critical infrastructure. In 2014, Congress passed several pieces of legislation in order to augment the cybersecurity workforce at DHS, including the Homeland Security Cybersecurity Workforce Assessment Act and the Border Patrol Agent Pay Reform Act. Among other effects, these laws expanded DHS's hiring authorities and allowed the Department to better recruit and hire qualified cyber professionals. Unfortunately, these new authorities have not yet been fully implemented.

Last month, the Government Accountability Office released a report entitled "Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements" – and the findings are troubling. While DHS has taken actions to identify, categorize, and assign employment codes to its cybersecurity positions, its efforts have been neither timely nor complete. Identifying DHS workforce capability gaps and recruiting to fill them is a problem this Committee has long examined; however, GAO found that DHS has not identified its department-wide cybersecurity critical needs. Ensuring that DHS collects complete and accurate data on all filled and vacant cybersecurity positions for identification and coding efforts is a task that DHS must not ignore or fail to complete. A scattershot approach to fulfilling workforce needs without comprehensive data to back those needs up is not an effective use of federal resources. In fact, there may even be the potential of delaying assistance to critical infrastructure sectors and state and local governments if DHS does not have an adequate amount of cyber workers with the correct skills.

At the same time, I am pleased to hear that DHS acknowledged and agreed with all of the recommendations presented by GAO in this report. DHS will create a periodic review process for cyber roles by the end of next month, and, most significantly, DHS promised to develop Department-wide guidance for identifying areas and positions of critical need by this summer. While DHS must work to overcome slow hiring processes and workforce pipeline issues in order to build the essential workforce required to meet its cyber mission, at the end of the day, DHS cannot bring people into the hiring pipeline if it does not have accurate accounting of what its current and future needs are.

NPPD is our government's premier civilian cybersecurity agency – a distinction that I hope will soon be bolstered by its elevation to the Cybersecurity and Infrastructure Security Agency with pending legislation in the Senate. So let us look at some of the challenges we will be discussing today as collective opportunities to lead together. We must get this right, and I believe that we will.

###